Alexandria Technical and Community College

CVNP 2625: Defensive Security

A. COURSE DESCRIPTION
   Credits: 4
   Lecture Hours/Week: 3
   Lab Hours/Week: 2
   OJT Hours/Week: *.*
   Prerequisites: None
   Corequisites: None
   MnTC Goals: None

   This course is designed to present a more advanced exposure to computer security for all users, from business professionals to students to home users. As computers and networks come under constant attacks today by hackers, computer security has become critical. This course provides a hands-on approach to computer and network security through discussion and a wide variety of tools used in the cyber-security field.

   Required hardware: Windows-based PC required with the operating system Windows 10 or higher. Chromebooks or other personal devices are not compatible with all required coursework. Required software: Office 365 or Office Professional 2019. Contact the instructor directly with any compatibility questions.

B. COURSE EFFECTIVE DATES:  04/15/2020 - Present

C. OUTLINE OF MAJOR CONTENT AREAS
   1. Explain the role of people in security.
   2. Understand how cryptography is used.
   3. Describe Public Key Infrastructure (PKI).
   4. Develop a plan for infrastructure security.
   5. Implement authentication and remote access.
   6. Understand wireless and mobile device security.
   7. Configure intrusion detection systems (IDS) and network security.
   8. Describe secure software development.
   9. Understand types of attacks and malicious software.
   10. Describe web components of security.
   11. Create a risk management plan.
   12. Develop an incident response plan.

D. LEARNING OUTCOMES (General)
   1. Describe the security threats facing modern network infrastructures.
   2. Understand how to secure a router; implement authentication, authorization, and accounting (AAA); mitigate threats to routers and networks using access control Lists (ACLs); and implement a secure network design (including management, and reporting),
   3. Understand how to mitigate common Layer 2 attacks, implement and administer a firewall, implement a site-to-site virtual private network (VPN) and implement a remote access VPN.

E. Minnesota Transfer Curriculum Goal Area(s) and Competencies
   None
F. LEARNER OUTCOMES ASSESSMENT
   As noted on course syllabus

G. SPECIAL INFORMATION
   None noted